State of North Carolina
Office of Information Technology Services

Michael F. Easley, Governor **George Bakolia, State Chief Information Officer**

Memorandum

To: George Bakolia

From: Ann Garrett

Subject: Recommendations for Statewide Information Security Manual Standards

Date: June 26, 2007

As part of the annual review of security standards required under GS 147.33.110, the Enterprise Security and Risk Management Office (ESRMO) reviewed the statewide security standards, industry standards and best practices and sought suggestions from other agencies subject to the standards. Based on the review, we recommend the following.

Security Policy and Standards Revision Recommendations

- Statewide password policies and standards:
  - Include and clearly define requirements by type of user (employees, contractors, vendors, business, citizens etc.).
  - Integrate statewide standards with the revised NCID policy.
- Statewide encryption policies and standards:
  - Check confidential data references and add requirements to protect personal identifiable information (PII).
  - Develop requirements for use of encryption for laptops, USB drives, and other mobile devices.
- Statewide business continuity policy and standards:
  - Include guidance with references for planning related to communicable diseases.
- Other Statewide Security Standards and Policies:
  - Review, reorganize, and update when necessary the 16 statewide policies and standards that are currently presented as a supplement to the Statewide Information Security Manual framework.

In addition, agency representatives provided the ESRMO with suggestions for additional training with regard to the Statewide Information Security Manual. Those recommendations follow:

P.O. Box 17209 • Raleigh, North Carolina 27619-7209
Tel: 919.981.5555 • Fax: 919.981.2548 • State Courier 51-01-11

Security Manual Training and Awareness Recommendations

- Agency suggestions for Statewide Information Security Manual training include:
  - How to use the statewide security manual.
  - How to obtain a Microsoft Word copy and search the manual.
  - How to locate and use security manual training materials on the security portal.
  - How to locate and use sample agency policies on the secure portal.
  - The legal and regulatory basis for the manual, as well as limitations to the scope of the manual to 'information technology standards'.
  - The ISO17799/2700X security standard and the ISO to NIST crosswalk.
- Annual security manual training has been moved to a date after December 31st in order to coincide with the security standards and policy review and approval cycle.

As part of the annual security standards review process a survey was distributed to state agencies. The detailed results and analysis that were used as input into these recommendations are attached.

Please let me know whether you agree with these recommendations and if you have any additional standards that you would like us to develop on your behalf. If you have any questions concerning these results and recommendations, please contact me at Ann.Garrett@ncmail.net or 919-981-5130.

cc: Bill Willis
Danny Lineberry

Attachment: Statewide Information Security Manual – Survey Results Analysis
Statewide Information Security Manual – Survey Results